WWW.SCIAM-MAGAZINE.NAROD.RU

Просеивание числового песка в поисках простых чисел

А.К. ДЬЮДНИ

ВОЗМОЖНО, из всех занимательных задач в теории чисел самая занимательная — это поиски простых чисел. Подобно золотым самородкам, они скрываются в «породе» остальных чисел. Напомним, что простое число — это то, которое не делится ни на какое другое, кроме 1 и на само себя. Такие числа редки. Правда, у самых истоков великой реки Континуума (множества всех чисел), пока числа еще невелики, они встречаются достаточно часто, но затем быстро растворяются в потоке, по мере того как величина чисел растет.

Существуют различные способы поиска простых чисел. Можно даже построить специальное просеивающее устройство, подобное промывным желобам, которые старатели применяют при поиске самородков, но так или иначе их приходится искать, потому что никто не знает, где они могут встретиться. Формулы для простых чисел не существует. Есть, правда, кое-какие геологические приметы, по которым можно искать их залежи. Так же как когда-то тысячи золотоискателей бросились в Калифорнию и на Юкон промывать песок в горных речушках в поисках крупинок желтого металла, так и наши читатели могут отправиться в страну чисел, но налегке, вооружившись лишь этим маленьким руководством.

Наверное, немногие математические понятия настолько доступны далекому от математики человеку, как понятие простых чисел. Любому встретившемуся на улице можно за минуту объяснить, что такое простые числа. Поняв, человек без труда напишет: 2, 3, 5, 7, 11, 13, 17 и т. д. Единица обычно не считается простым числом.

Возможно ли распознать простое число, как говорится, с первого взгляда? Если вы зачерпнули в сито сразу много чисел, сверкнет ли среди них простое, как золотой самородок? Некоторые считают, что да. Например, числа, оканчивающиеся на 1, часто оказываются искомыми, скажем, такие как 11, 31, 41. Однако при этом следует быть осторожным и не принять фальшивое золото за чистое, как, скажем, 21 или 81. По мере роста величины чисел, единица на конце все чаще вводит нас в заблуждение. Создается даже впечатление будто простые числа в конце концов просто исчезают, как полагали некоторые древние греки. Существует ли последнее, самое большое по величине простое число? Первое дошедшее до нас доказательство того, что конца простым числам не существует, принадлежит Евклиду.

Доказательство настолько простое, что его можно представить в виде диалога в стиле Сократа, который Евклид ведет с рабом. Однако мне больше нравится беседа между новичком и старожилом, которые встретились на берегу великой реки Континуум:

НОВИЧОК: Эй, мистер! Как далеко вниз по течению заходят простые числа?

СТАРОЖИЛ: До самого моря Бесконечности, парень.

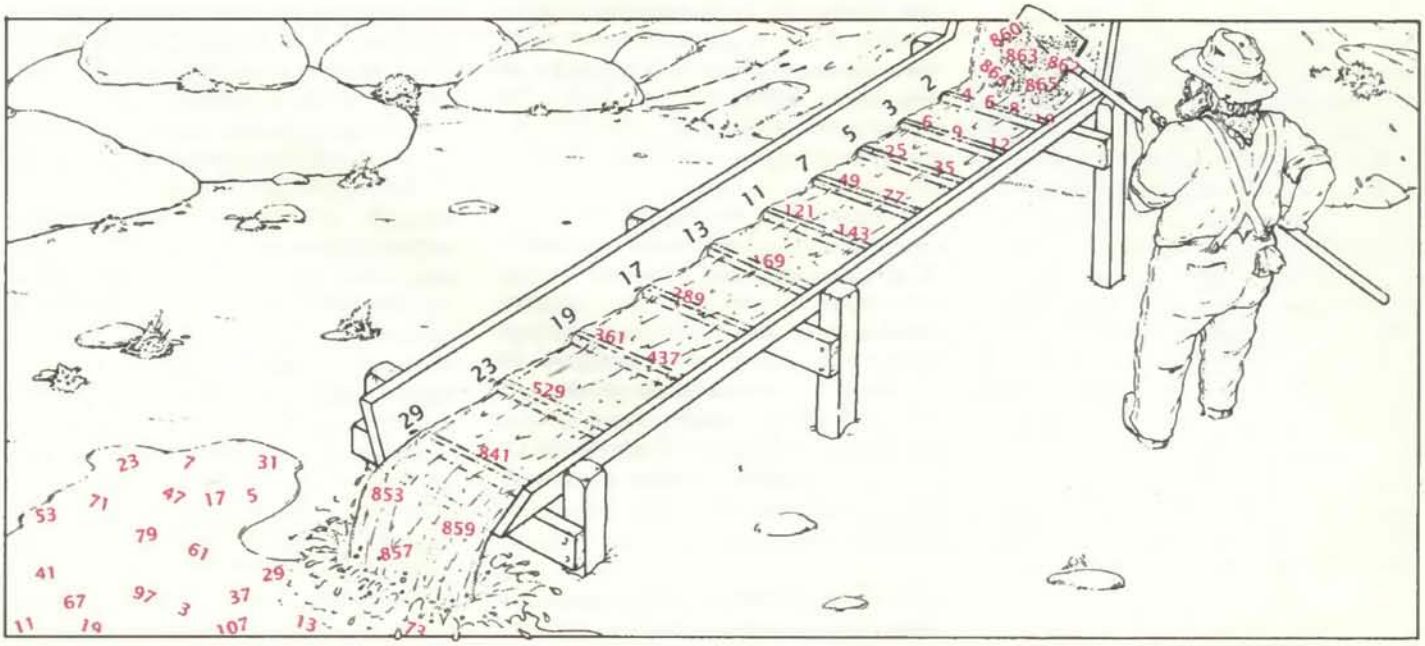
НОВИЧОК: Я вам не верю. Мы здесь на уровне миллионов, а мне еще ни разу не повезло за целый день.

СТАРОЖИЛ: Эх, молодежь, вам нужно все объяснять! Смотри, допустим, ты дошел до последнего простого числа. После него их уже не существует, так?

НОВИЧОК: Ну, так.

СТАРОЖИЛ: Назовем его n. Составим произведение из всех простых чисел вплоть до n. Это будет $2 \times 3 \times 5 \times 7 \times \ldots \times n$. Теперь прибавим к произведению 1 и назовем это число p.

НОВИЧОК: И что же, вы хотите сказать, что p — простое число?



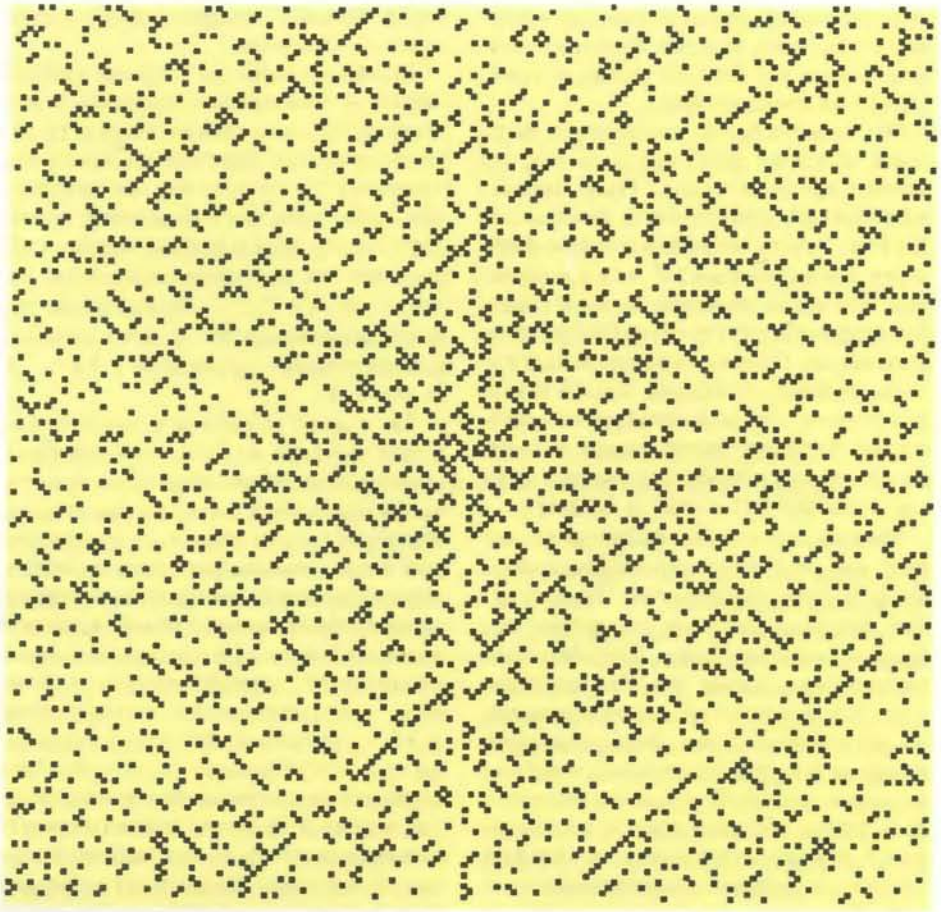
Промывочный желоб для поиска простых чисел

WWW.SCIAM-MAGAZINE.NAROD.RU

СТАРОЖИЛ: Конечно. Простое — проще некуда. Смотри, ты не можешь разделить его на 2, потому что остается 1. Ты не можешь разделить его на 3, потому что остается 1. Каждый раз всегда остается 1, вплоть до n. Ее никак не обойдешь.

НОВИЧОК: Вот оно что! Значит, вы правы, им конца нет.

СТАРОЖИЛ: Так-то вот. Ну ладно, чего стоишь без дела, помоги-ка мне с этим промывным желобом.



Спираль Станислава Улама выявляет несколько месторождений простых чисел

Хотя самого большого простого числа не существует вообще, но самое большое простое число из тех, что нам известны, все же есть. Это различие непонятно некоторым читателям и даже журналистам. Вся беда заключается в этих заголовках на последней странице газет и журналов: НАЙДЕНО САМОЕ БОЛЬШОЕ ПРОСТОЕ ЧИСЛО. Иногда эта путаница продолжается и в самом газетном сообщении, из которого мы узнаем, например, что с помощью нового суперкомпьютера только что удалось доказать, что число, содержащее 7067 знаков, а именно $5 \times 2^{23473} + 1$ является простым. У него нет делителей, кроме 1 и, конечно, самого себя. В сообщении может отсутствовать напоминание (или читатель может проглядеть его) о том, что это лишь самое большое из известных простых чисел, и что вскоре, возможно, будет найдено новое, еще большее простое число.

Я затрудняюсь сказать, каково максимальное простое число из известных на сегодняшний день. Возможно, к тому времени, как эта статья выйдет в свет, оно уже будет другим. Ну а на тот момент, когда я писал эти строки, наибольшее простое число состояло из 65050 разрядов и было найдено Дэвидом Словински из фирмы Cray Research, Inc. в 1985 году: $2^{216091} - 1$. Простые числа, имеющие форму $2^m - 1$, называются числами Мерсенна, в честь французского математика-любителя Марена Мерсенна. Другой любитель С. Йетс из Делри-Бич (шт. Флорида) собрал в своей коллекции все известные простые числа, большие 1000. Его коллекция полна и точна.

Насколько быстро простые числа разрежаются по течению реки Континуума? Из первых 10 чисел 4 являются простыми, таким образом их доля составляет 40%. В первой сотне их содержание падает до 25%, и оно продолжает падать с ростом величины чисел более или менее регулярно. В общем количество простых чисел до n включительно приблизительно равно $n/\log n$. (В данном случае это приближение является асимптотическим. Другими словами, если количество простых чисел, меньших для равных n, обозначить $p(n)$, то отношение $p(n)$ к величине $n/\log n$ все ближе приближается к 1, по мере того как n становится все больше и больше. Таким образом, вниз по течению Континуума простые числа разрежаются пропорционально натуральному логарифму от n.)

Давайте посмотрим, как действует это правило, подставив в формулу несколько пробных значений n. Например, сколько простых чисел содержится в интервале от 1 до 100 и в интервале от 1 до 1000? В первом случае формула дает что-то около 22, во втором — около 145.

Неудивительно, что это явление постепенного разрежения дает все более длительные интервалы, вовсе не содержащие простых чисел. Например, чтобы найти отрезок длиной в миллион, не содержащий ни одного простого числа, нужно лишь проплыть вниз по течению, как это однажды сделал Мартин Гарднер, до числа 1000001! Здесь восклицательный знак поставлен не для того, чтобы выразить восхищение или удивление: он означает число, равное $1 \times 2 \times 3 \times \ldots \times 1000001$. Как говорят дети, число, конечно, «здоровущее». Однако нетрудно убедиться, что с этого числа начинается интервал, не содержащий ни одного простого числа. Если в формуле $1000001! + n$ число n пробегает последовательные значения от 2 до 1000001, то каждое из получаемых чисел является составным. Потому что в любом случае $1000001!$ делится на n, и n делится на себя, т. е. число $1000001! + n$ делится на n.

Я уже говорил, что для простых чисел не существует никакой формулы, никакой комбинации алгебраических операций над n, выполняя которые можно было бы получить очередное, n-ое простое число. Многие люди впадали в заблуждение на этот счет, достигнув некоторых первоначальных успехов. Хорошо иллюстрирует подобные заблуждения шуточная поговорка, известная любому студенту-математику. В ней говорится о трех способах «доказательства» того, что все нечетные числа простые:

МАТЕМАТИК: 3 — это простое число, 5 — простое, 7 — простое ..., а дальше доказательство по индукции.

ФИЗИК: 3 — простое число, 5 — простое, 7 — простое, 9 — ошибка эксперимента, 11 — простое ...

ИНЖЕНЕР: 3 — простое число, 5 — простое, 7 — простое, 9 — простое ...

Инженер, как говорится, может

WWW.SCIAM-MAGAZINE.NAROD.RU

смеяться последним, поскольку математики в своих поисках больших простых чисел все больше должны полагаться на компьютеры.

Но, может быть, существует формула, которая дает, пусть не все, но только простые числа? Пьер Ферма, знаменитый французский математик XVII в., думал, что нашел такую формулу, когда написал $2^{2^n} + 1$. Он полагал, что какое значение ни подставь в эту формулу, результатом будет простое число. Однако этот мыльный пузырь, пущенный Ферма, лопнул после его смерти, когда швейцарский математик Леонард Эйлер нашел делители для пятого «простого числа» Ферма: $4\,294\,967\,297 = 641 \times 6700417$.

Иногда своего рода формула возникает как результат наблюдения визуальных закономерностей. Одну из таких закономерностей случайно открыл Станислав Улам, американский математик, поляк по происхождению. Сидя как-то на скучной лекции, он, ни о чем не думая, начал рисовать решетку из горизонтальных и вертикальных линий. В одной из полученных таким образом клеток он поставил 1 и стал нумеровать остальные клетки по спирали, расходящейся от первой клетки:

5 4 3
6 1 2
7

Когда спираль совершила уже несколько оборотов, Улам начал обводить кружками простые числа, не преследуя никакой определенной цели. Однако вскоре заметил, как на его глазах возникает довольно любопытная закономерность. Откуда ни возьмись, стали появляться прямые линии. Улам, конечно, сразу понял, что такие линии говорят о закономерности, которую можно облечь в формулу для простых чисел. Компьютерная распечатка, приведенная на с. 83, дублирует то, что Улам сделал от руки. На компьютерном графике составные числа представлены маленькими белыми квадратиками, а простые — черными.

Выделяющиеся на графике темные линии — это залежи простых чисел. Каким образом можно выразить эту геологическую картину на языке математики? У самого центра диаграммы одно такое месторождение пролегает сверху вниз и справа налево. Оно состоит из последовательности чисел: 7, 23, 47, 79... . Оказывается, эту последовательность можно описать квадратичной функцией $4x^2 + 4x - 1$.

Те, у кого остались в памяти кое-какие сведения из школьной алгебры, смогут подобрать формулы практически для любой линии на диаграмме. Формула может оказаться справедливой и для множества простых чисел, лежащих далеко за пределами приведенной диаграммы. Эйлер, который так многим не дал сделать карьеру в математике, предвосхитив множество математических результатов, тоже «открыл» аналогичную формулу еще в XVIII в.: $x^2 + x + 41$. Эта формула не видна на диаграмме Улама, чтобы ее увидеть, нужно в качестве начального числа спирали выбрать другое значение. Если начать спираль с 41, то мы получим месторождение, содержащее сразу 40 последовательных простых чисел!

Но, наверное, с помощью формул простые числа ищут лишь дилетанты. Опытные старатели, работающие на берегах реки Континуума, предпочитают решето, а еще лучше промывные желоба. С одного конца в эти устройства загружаются всевозможные числа, а с другого конца из него выходят только простые числа. Специальные фильтры улавливают составные числа при помощи проверки на делимость (см. рисунок на с. 82). Разумеется, такие промывные желоба очень хорошо работают в компьютерах.

Простейшие фильтрующие устройства отделяют простые числа путем деления на 2, 3, 4 и т. д. Если ввести в устройство число n, оно проверяет его делением на 2, на 3, на 4 и продолжает проверки до тех пор, пока одна из них не окажется успешной или делитель не достигнет n. В первом случае число составное, во втором — простое. Алгоритм модели промывного желоба может послужить основой простейшей программы для домашнего компьютера. Назовем этот алгоритм SLUICE1:

```
input n
f ← 1
for k ← 2 to n − 1
  test ← rem (n/k)
  if test = 0 then f ← 0
  if f = 1 then output «простое»
```

На входе программа принимает число n, вводимое человеком с клавиатуры. Затем программа устанавливает у переменной f (действующей как флажок) значение 1. Если f все еще равно 1, когда программа завершает свои вычисления, значит, число является простым. В теле цикла многократно повторяется один условный оператор *if*. Индекс k пробегает значения от 2 до $n - 1$. Для каждого значения k программа выполняет деление n/k, берет остаток от деления (rem) и запоминает его под именем *test*. Чаще всего значение *test* оказывается ненулевым, другими словами, k не делит n без остатка. Но если хоть раз оно оказывается нулевым, программа немедленно сбрасывает флажок f, записывая туда 0, и это значение сохраняется вплоть до конца цикла. Если условие во втором операторе *if* удовлетворяется, программа печатает «простое». Если же f было установлено в нуль где-то по ходу выполнения цикла, то программа хранит мрачное молчание.

Хотя описанная выше программа очень проста, она работает слишком медленно, особенно если заставить ее найти несколько простых чисел подряд. Для этого нужно лишь заменить первый оператор *input* оператором цикла, таким, например, как «for $n \leftarrow$ $\leftarrow$ 3 to 1000». А последний оператор в программе можно изменить так, чтобы вместо «простое» печаталось очередное значение n, успешно прошедшее все проверки и ни разу не разделившееся без остатка. Мы увидим, как начнут появляться простые числа от 3 до 997, по одному и очень медленно.

Однако работу программы SLUICE1 можно значительно ускорить, если внести в нее кое-какие изменения. Во-первых, не имеет никакого смысла проверять, делится ли число n на k, если k больше квадратного корня из n, потому что по крайней ме-

67	1	43
13	37	61
31	73	7

3	61	19	37
43	31	5	41
7	11	73	29
67	17	23	13

Магические квадраты из простых чисел: Генри Эрнеста Дьюдни (слева) *и Аллана У. Джонсона-мл.* (справа)

3	1	3	9	9	1
9	8	3	9	2	9
1	6	4	3	1	2
5	1	7	4	7	1
7	1	5	9	7	1
9	3	7	3	3	9

Решетки простых чисел 6 × 6 *Гордона Ли*

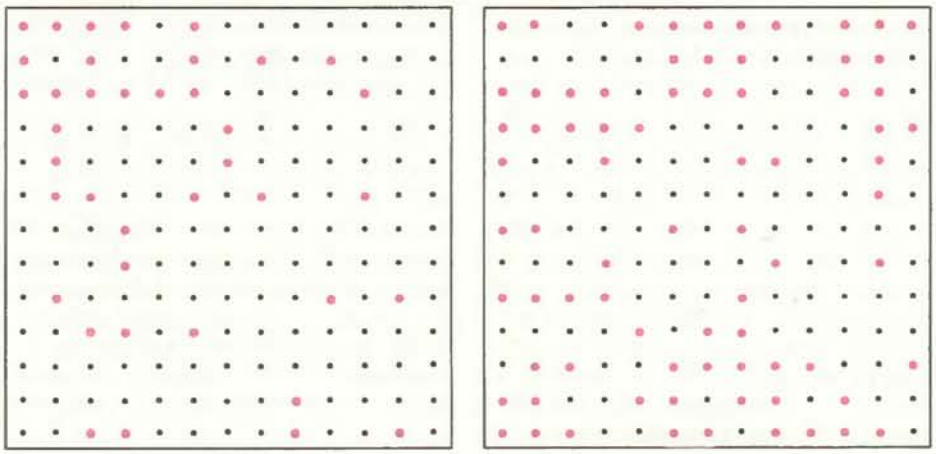
WWW.SCIAM-MAGAZINE.NAROD.RU

ре один делитель числа n, если он есть, не должен превосходить квадратного корня из n, а одного делителя уже достаточно, чтобы считать число составным. Существует также знаменитая арифметическая теорема, которая гласит, что любое целое число можно представить в виде произведения простых чисел, и это произведение единственное. Число не является составным, если оно не делится ни на одно простое число, меньшее себя. С учетом обоих этих фактов цикл можно сделать значительно короче, выбирая в качестве значений индекса k только простые числа, не превосходящие по величине квадратного корня из n.

Новый алгоритм, который мы назовем SLUICE2, в достаточной мере отличается от своего незамысловатого предшественника и выглядит следующим образом:

```
r ← 1
p(1) ← 2
for n ← 3 to 1000
  k ← 1
  f ← 1
while f = 1 and p(k) ≤ sqrt(n)
  test ← rem (n/p(k))
  if test = 0 then f ← 0
  k ← k + 1
if f = 1 then r ← r + 1
  p(r) ← n
```

Поскольку программа SLUICE2 требует списка простых чисел, она запоминает каждое новое простое число в специальном массиве p. Переменная k является индексом, указывающим на последний элемент p. Таким образом, программа всегда знает, куда поместить следующее полученное ею простое число. В первой строке алгоритма индексу присваивается значение 1. В следующей строке в первый элемент массива простых чисел p помещается число 2. Затем следует цикл, описанный выше. В нем проверяются все числа в диапазоне от 3 до 1000. Переменная k указывает, какой элемент массива p используется в данный момент для проверки n. Внутри этого основного цикла есть еще один цикл типа *while* — пока флажок f равен 1 и очередное простое число из массива p не превышает квадратного корня из n, внутренний цикл продолжает проверки, выбирая последовательные значения k. При выходе из этого цикла флажок f может быть равен либо 1, либо 0. В первом случае это означает, что было найдено еще одно простое число. Программа добавляет его к уже существующему списку. Во втором случае в основном цикле просто произойдет переход к следующему значению n.



Прореагировавшие матрицы: Д. Фэкса (слева) *и П. Кейна* (справа)

Читатели, которые пожелают воспользоваться этим вариантом программы поиска простых чисел, могут выбрать один из двух способов вывода найденных значений. Программа SLUICE2 может распечатать весь массив p по завершении главного цикла алгоритма. При этом вы как бы увидите полное решето самородков. Но, может быть, вам больше понравится наблюдать, как самородки появляются по одному, как только они будут найдены. В таком случае сразу после оператора $p(r) \leftarrow n$ нужно вставить оператор печати *print*.

Возможно, предложенный диапазон поиска, от 1 до 1000, покажется читателям слишком маленьким. В принципе ничто не мешает увеличить верхний предел поисков до 100 000 или даже до 1 000 000. А может быть, что-то все-таки помешает? Это будет зависеть от того, насколько большие массивы допускаются в том или ином компьютере. Размер основного массива программы определяется количеством простых чисел, которые должны быть найдены по ходу выполнения программы. Здесь нам пригодится формула, оценивающая количество простых чисел. Согласно этой формуле, в диапазоне от 1 до 1 000 000 содержится приблизительно 72 382 простых числа. Если память компьютера имеет размер лишь 64 Кбайт, то он не справится с этой задачей.

Простым числам было посвящено множество занимательных математических задач. Продолжая тему простых чисел в применении к квадратным матрицам, рассмотрим две задачки. Первая из них была придумана Генри Эрнестом Дьюдни, известным английским специалистом по головоломкам. Наверное, многим читателям уже знакомы так называемые магические квадраты — квадратные матрицы чисел, у которых суммирование элементов по любой строке, любому столбцу и двум главным диагоналям дает одно и то же число. Существуют ли магические квадраты, состоящие только из простых чисел? Оказывается, да. Магический квадрат размером 3 × 3, приведенный на с. 84, имеет сумму 111 (между прочим, тоже не простое число) вдоль каждой строки, каждого столбца и каждой главной диагонали. Рядом с этой матрицей 3 × 3 приведена матрица 4 × 4. Известны магические квадраты и со стороной больше 4. Мы просим читателей, которым удастся самостоятельно открыть такие квадраты, прислать нам свои результаты. Лучшие из них будут опубликованы в одной из наших следующих статей. Результат будет тем ценнее, чем больше размер квадрата, а при одинаковых размерах преимущество будут иметь квадраты с меньшими суммами.

Другую задачку предложил еще один неутомимый английский изобретатель головоломок Гордон Ли, автор рубрики «Победители и побежденные» в журнале «Dragon User». Он построил квадрат 6 × 6, состоящий из цифр, которые скрывают в себе великое множество простых чисел, а точнее говоря, 170 (см. правый рисунок на с. 84). Простые числа по диаграмме Ли можно строить из цифр любой строки, любого столбца и любой диагонали, просматривая их в произвольном направлении. Несколько полученных таким образом цифр могут составлять простое число, одно из 170, по подсчетам Ли. Всего в решетке размером 6 × 6 содержится максимум 616 чисел (как простых, так и составных). Повторяющиеся простые числа считаются как одно число. В своих подсчетах Ли включил в список простых чисел и 1.

Интересно, а смогут ли читатели составить свой квадрат из цифр размером 6 × 6, который содержал бы больше 170 простых чисел? Те, кто напишет и выполнит программы SLUICE1 и SLUICE2, получат некото-

WWW.SCIAM-MAGAZINE.NAROD.RU

рое преимущество перед остальными участниками этого конкурса. Ли подсказывает, что по квадрату должны быть рассеяны цифры 1, 3, 7 и 9, поскольку простые числа оканчиваются всегда на одну из этих цифр. С другой стороны, если составить квадрат только из этих цифр, он, как ни странно, окажется довольно бедным на простые числа. Разумно разбросав четные числа, включая 0, можно увеличить свои шансы в попытках превзойти результат Ли. Я опубликую лучшее из присланных решений (конечно, если оно содержит более 170 простых чисел).

В МАЙСКОМ номере журнала мы говорили о домашней компьютерной лаборатории, в которой моделировались эффекты давления с помощью молекул газа, сталкивающихся со стенками замкнутого сосуда. Молекулы участвовали также в процессе цифровой диффузии, распространяясь от одного края сосуда к другому. Наконец, атомы опасного нестабильного вещества, названного мною гридием, были собраны в критическую массу. Некоторые читатели построили свои собственные сосуды, содержащие газ под давлением, и свои диффузионные камеры, но большинство, конечно, заинтересовались гридием. Со всей Северной Америки, а потом и из других частей света посыпались на мой стол доклады о «компьютерных взрывах».

Описав путь испускаемого при делении нейтрона линейным уравнением, я тем самым неявно предполагал, что два нейтрона, удаляясь от расщепленного атома, должны двигаться в противоположных направлениях. Большинство читателей, однако, выбрали лишь одно из этих направлений. Так или иначе, расщепить все атомы плоской решетки размером $h \times n$ оказалось весьма непросто.

Построив по результатам многочисленных экспериментов диаграмму, Р. Касл из Уэбстера (шт. Техас), установил, что в решетке размером 16 × 16 обычно реагирует 90% атомов. А когда размер решетки достигает 32, количество делящихся атомов достигает уже 99%. Р. Мартин, профессор философии Университета Далузи в Новой Скотии, пришел к следующим результатам: когда размер решетки равен 19, реагирует 90% атомов, а при размере 39 количество прореагировавшего материала достигает уже 99%. Большинство других ядерных экспериментов дали результаты, укладывающиеся в этот диапазон. Среди тех читателей, кто воспользовался моделью с двумя нейтронами, был, например, Р. Смит из Энн-Арбора (шт. Мичиган). Он пришел к типичным результатам с меньшей критической массой. Согласно его данным, в решетке 15 × 15 реагирует 98% атомов.

Наверное, немногим читателям удалось создать такую сложную и совершенную систему, какую представляет собой программа SHAKEY, написанная Р. Меркином из Нортэмптона (шт. Массачусетс). Программа SHAKEY не только управляется с очень большими решетками, но и с помощью многих приемов, позволяющих сэкономить время, работает очень быстро. Домашний реактор SHAKEY позволяет экспериментировать с различными интервалами в решетке, а также отмечает каждый распад звуковым сигналом, щелкая подобно счетчику Гейгера. Меркин пишет, что готов с удовольствием поделиться своей программой со всеми желающими.

Изображения взорвавшихся решеток, приведенные на рисунке вверху, были присланы Д. Фэксом из Питтсбурга (шт. Пенсильвания) и П. Кейном из Шампейна (шт. Иллинойс).

Наука и общество

Финансирование науки: от кого оно зависит?

В МАЕ на «вашингтонском небосводе» расположение звезд, определяющих судьбу науки, было неблагоприятным. Стечение двух обстоятельств — закат власти нынешнего президента и полученное в декабре прошлого года согласие конгресса относительно ограничения бюджетных ассигнований на внутренние нужды в новом финансовом году — привело к тому, что нескольким проектам из области «большой науки» был нанесен серьезный удар на Капитолийском холме. Один из подкомитетов палаты представителей проголосовал за то, чтобы отложить строительство всех новых объектов, которое должно было начаться в 1989 г., в том числе сверхпроводящего суперколлайдера SSC и фотонного излучателя «Advanced Photon Light Source», который стоит 456 млн. долл. и предназначен для генерирования синхротронного излучения в экспериментальных исследованиях, связанных с разработкой новых материалов. Представленная сенатом предварительная структура бюджетных ассигнований была расценена некоторыми конгрессменами и их советниками как симптом надвигающейся опасности; так, например, если она будет принята, придется прекратить все работы по строительству космической станции. Предложения сената означают также, что Национальный научный фонд (ННФ), который финансирует многие гражданские исследования в области фундаментальных наук и бюджет которого администрация планировала удвоить в ближайшие пять лет, будет рад получить хоть какую-нибудь прибавку к ассигнованиям.

Научная общественность выражает свое недовольство. Руководители исследовательских лабораторий, включая Брукхейвенскую национальную лабораторию и Станфордскую лабораторию синхротронного излучения (СЛСИ), заявляют, что вследствие сокращения бюджетных ассигнований имеющееся у них научное оборудование используется далеко не в полной мере. Директор СЛСИ А. Бьененсток сказал, что у них имеется «установка, которую они не могут использовать», хотя на ней можно было бы выполнять важные работы по проекту нового фотонного излучателя. А. Шрисхайм, руководитель Аргонской национальной лаборатории, которая недавно была объявлена центром по разработке новых высокотемпературных сверхпроводников для промышленных целей, заявил, что дополнительные 2 млн. долл., выделенные в этом году на указанные работы, «не покроют основного дефицита». Директор управления по обслуживанию обсерваторий при Национальной организации радиоастрономических обсерваторий Р. Хавлен считает, что недостаток средств породил ряд проблем в отношении работы системы VLA (большой антенной решетки) в Нью-Мексико, «настолько острых, что, по-видимому, придется отказаться от некоторых астрономических наблюдений».

Что же делать в такой ситуации? На ежегодном заседании Национальной академии наук ее президент Ф.Пресс, бывший советник по науке при президенте Дж. Картере, внес ра-